E-mail Management

Overview

E-mail messages most often include official government records, so you should include e-mail as part of your electronic records management strategy. The medium is irrelevant. The content of the message determines whether it is a record or not; the content determines to which records series the message belongs; and the content determines how long the message needs to be retained.

Both statute and case law make clear that government agencies have to include e-mail in an overall records management strategy. Currently, few government agencies manage e-mail as records. Managing e-mail is usually left to personal preference or routine systems back-ups and administrative procedures that treat all e-mail alike. These practices can result in serious legal, operational, and public relations risks. As well, staff must be persuaded of the need to file, protect and maintain access to e-mail records.

Legal Framework

For information on the legal framework you must consider when developing an e-mail records management policy, review the requirements of the:

- Wyoming Public Records Act – WPRA (Wyoming Statutes 16-4-201 through 16-4-205) (available at: < http://legisweb.state.wy.us/statutes/titles/title16/c04a02.htm >), which:
    - Mandates that government agencies must keep records to fulfill the obligations of accountability and stipulates that the medium must enable permanent access.
    - Stipulates that you can copy a record and that the copy, if trustworthy, will be legally admissible in court. This stipulation means that you can copy your e-mail messages to paper or to text files, as long as the record's content, context, and structure are intact.
    - Does *not* differentiate among media. The *content* of the e-mail message determines whether the message is a record.
- Wyoming Statutes 9-2-401 through 9-2-419 which:
    - Defines a public record as the original and all copies of any paper, correspondence, form, book, photograph, photostat, film, microfilm, sound recording, map, drawing or other document, regardless of physical form or characteristics, which have been made or received in transacting public business by the state, a political subdivision or an agency of the state.
    - Classifies public records
    - Transfer of public records to the WSA.

  - Provides for the designation of a records office in each state department or agency.
  - Records are the property of the state.
  - Procedures for the destruction and disposition for public records.

- Uniform Electronic Transactions Act (UETA) (Wyoming Statutes, 40-21-101 through 40-21-119) (available at: < http://legisweb.state.wy.us/statutes/titles/title40/CHAPTER21.htm >) and Electronic Signatures in Global and National Commerce (E-Sign), a federal law (available at: < http://thomas.loc.gov/cgi-bin/query/z?c106:S.761: >). Both UETA and E-Sign address the issue of the legal admissibility of electronic records created in a trustworthy manner and address the issue of applying a paper-oriented legal system to electronic records.

- Executive Branch Electronic Mail Policy (Executive Department, Executive Order - 1999-4) (available at: <http://www.state.wy.us/governor/press_releases/execorder/1999/pre1999-4.html >) Provides the minimum requirements for e-mail usage and management.

Additional Legal Considerations

Within the context of these laws, you should also consider:

- *The ramifications of the* Armstrong *litigation*. In Armstrong v. Executive Office of the President (1 F.3d 1274 [DC Cir 1993]), a federal court found in favor of a group of researchers and nonprofit organizations who wanted to prevent the destruction of e-mail records created during the Reagan administration. The court determined that federal government agency e-mail messages, depending on content, *are* public records and that complete metadata must be captured and retained with the e-mail record. Although a federal decision, this litigation has strongly influenced government agencies at all levels. Other agencies are now paying closer attention to their e-mail records management practices, including the capture of metadata.

- *Legal discovery*. When developing your policy, balance your legal and operational requirements with the risk of being engaged in legal discovery. You must meet all government requirements for managing your e-mail records, but you should also be able to respond to discovery in an affordable, efficient, and practical way. Bear in mind that many courts have upheld discovery requests for e-mail records. For more information on the discovery of electronic records, refer to Appendix E of the *Trustworthy Information Systems Handbook*.

Key Concepts

As you develop your e-mail records management policy, you will need to be familiar with the following key concepts:

- Goals of your process
- E-mail policy components
- Training for staff members
- Recommended process for e-mail policy development

Goals of Your Process

Though your agency will develop unique procedures that meet your specific operational and legal requirements, bear in mind the following goals for an e-mail record. An e-mail record should be:

- *Complete*. E-mail records should completely document the transaction. For example, you cannot save just the text and none of the sender information. Complete e-mail records must include all of the following elements, as applicable:
  - Recipient(s)
  - Sender
  - Subject
  - Text
  - Date sent
  - Time sent
  - In cases were attachments are not retained as the record copy elsewhere, complete attachment(s), which should be included in full (not just indicated by file name), because the attachment is part of the record. If the record copy of the attachment is retained elsewhere, the complete file name of the attachment should be included in the body of the e-mail.
  - Group list members, so that if an e-mail record simply lists the group name in the recipient field, the recipients can be identified. For example, the group list "HR" (a group list for all the members of the human resources department) should be documented so that each member of the list is named.
  - Directory of e-mail addresses and the corresponding staff member names (e.g., jado25@myorg.net is Jane Doe), so that an e-mail address listed in an e-mail record can be linked to a person
- *Accurate*. The contents of the e-mail record should accurately reflect the transaction.
- *Accessible*. Some e-mail records must be accessible to the public and some should not be publicly accessible, depending on the content of the record and as determined in the WPRA. All e-mail records, like other electronic records, should be reasonably accessible for the purposes of legal discovery.
- *Manageable*. The e-mail record should be easy for staff members to manage as part of the daily workflow and records management practices. Because you will rely on staff members

to implement and use the e-mail records management policy, procedures should be straightforward.

- *Secure*. The e-mail record should reside in a secure system that controls access, storage, retrieval, alteration, and deletion. This goal is particularly important to control access to restricted e-mail records, as set forth in the WPRA. E-mail records present unique security concerns, because e-mail messages are:
  - Easily manipulated or deleted in the system
  - Easily captured and read by unintended persons
  - Easily forwarded and misdirected by mistake

E-mail Policy Components

The Executive Branch Electronic Mail Policy (Executive Department, Executive Order - 1999-4) provides the minimum standard for e-mail usage and management. Should your agency choose to implement your own policy, the components of an e-mail retention policy should at a minimum include:

- *Confidentiality*. Include provisions for maintaining confidentiality of restricted records.
- *Assignment of ownership*. Clearly communicate that both the sender and the receiver should save e-mail records to document transactions and responsibilities completely. For example, if Person A sends an e-mail message to Person B with important information that affects agency policy, the transaction includes not only Person A's sending of the information, but Person B's receipt of the information.
- *Process for retention*. Guide staff members in determining which e-mail messages are records. Also, outline a procedure for grouping e-mails into records series, and a records retention schedule created for each series as mandated in the WPRA.
- *Process for managing*. Include procedures for organizing, storing, maintaining, accessing, and disposing of e-mail records. Also, establish a procedure for documenting your e-mail records policy, including the software and hardware in use, specific procedures, training efforts, staff member responsibilities, and records retention schedules.
- *Summary of responsibilities*. Make clear the records management responsibilities of staff members and groups (e.g., departments, project teams, committees) as they engage in their daily work.

Training for Staff Members

Staff members will need to be trained on how to answer legal and operational questions about e-mail. Your training and documentation material should set forth guidelines that staff members can follow to answer such questions in the course of their work. Possible questions include:

- Is this e-mail an official record? Is this e-mail message administrative or personal (e.g., “Thursday staff meeting to start an hour late.” or “Let’s do lunch!”)?
- Does this e-mail message have long-term significance (e.g., “New policy finalized.”)? Does this e-mail message document a transaction or operations function (e.g., a process, a decision, or a discussion)?
- Is this e-mail record public or restricted as set forth by the WPRA?
- What metadata must I capture when I save this e-mail record?
- Which records series does this e-mail record belong in?
- Should I save the complete e-mail record, including attachments and group list names?
- Could this e-mail message ever be required as evidence in a legal action?

Recommended Process for E-mail Policy Development

Should your agency choose to implement your own policy, use the following steps to guide you as you develop your e-mail records management policy:

1. Identify and organize key stakeholders in your organization.
2. Draft the policy and process with the input of key stakeholders.
3. Meet with key stakeholders, including individual staff members.
4. Finalize the policy with the input and support of key stakeholders.
5. Implement the policy technically by setting up and testing the procedures.
6. Train the staff members on the new procedures. (Training is especially important because you must rely on staff members to ensure the integrity of the procedures.)
7. Implement the policy for staff members on a planned schedule.

On an on-going basis, from initial development to future policy changes, document the development of your e-mail records management policy, the policy itself, and changes to the policy.

Key Issues to Consider

Now that you are familiar with the operational and legal importance of managing e-mail messages as records, you can use the questions below to begin the development of your e-mail management policy. Discussion of the questions below will help:

- Did you ensure that you meet your legal and operational requirements
- Was staff member input, support, and compliance gathered as part your e-mail management policy
- Did you integrate your records management policy with your overall electronic records management strategy
- Did you establish procedures to ensure that staff members manage e-mail records at the appropriate points in the records continuum, rather than as a single records series with one retention schedule.

Discussion Questions

- How can we ensure staff member compliance and understanding? What process is reasonable to ask staff members to comply with?
- How should we train staff members? How accountable should we make staff members for compliance?
- How should we develop our process?
- How do we train staff to recognize which e-mail should be retained as a record?
- What elements of an e-mail record do we need for a complete understanding of the transaction?
- What is the appropriate records series and records retention schedule for each records series? How should e-mail records be organized for long-term storage and access (e.g., project, department, function)? How will we retrieve and dispose of e-mail on our chosen storage media?
- How should our e-mail retention strategy coordinate with our other records management procedures (e.g., store all project-related e-mail with the other project documentation)? What documentation do we need for our process?
- How should we implement the procedures technically and operationally? How can we plan our implementation so the policy is widely used and accepted, but causes minimal disruption to our daily operation? Annotated List of Resources

Primary Resources

Ginn, M.L. *Guideline for Managing E-mail*. Prairie Village, KS: ARMA International, 2000.

Topics covered in this overview of e-mail management include organizational issues (e.g., legal, operational, governmental), creation and use of e-mail, and management of e-mail as a record (including filing, classification, backup, and disaster recovery).

Minnesota Historical Society, State Archives Department. *Trustworthy Information Systems Handbook*. Version 2, August 2000.
< http://www.mnhs.org/preserve/records/tis/tis.html >

This handbook provides an overview for all stakeholders involved in government electronic records management. Topics include ensuring that information systems are accountable to elected officials and citizens by developing systems that create reliable and authentic information and records. The handbook provides an overview of the characteristics that define trustworthy information. The handbook also provides a series of worksheets for evaluating and refining a system to ensure trustworthy information.

Wallace, D.A. *Recordkeeping and Electronic Mail Policy: The State of Thought and the State of the Practice*. Proceedings of the Annual Meeting of the Society of American Archivists, September 3, 1998, Orlando, FL. Arlington, VA: Barry Associates; 1998:1–23.
<http://www.rbarry.com/dwallace.html >

This paper summarizes the issues surrounding e-mail policies and records management strategies. The paper describes e-mail records management policy elements and discusses the tasks and key concerns associated with the development of an e-mail records management policy.

Additional Resources

Utah State Archives and Records Services, Electronic Records. Salt Lake City, UT: Utah State Archives and Records Services, State of Utah, 2001.
<http://www.archives.state.ut.us/recmanag/electronic.htm >

Visit this web site for links to the e-mail policies of a number of states in the United States, as well as links to additional web resources for records management.

Special thanks to the Minnesota State Archives for their help in the development of this guide.